(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 November 2001 (01.11.2001)

PCT

(10) International Publication Number
WO 01/82092 A1

(51) International Patent Classification[7]: G06F 15/00

(21) International Application Number: PCT/AU01/00451

(22) International Filing Date: 19 April 2001 (19.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PQ 7042 20 April 2000 (20.04.2000) AU
PQ 7974 6 June 2000 (06.06.2000) AU

(71) Applicant *(for all designated States except US)*: **AUSTRALIA AND NEW ZEALAND BANKING GROUP LIMITED** [AU/AU]; 100 Queen Street, Melbourne, VIC 3000 (AU).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **DANKS, David, Hilton** [AU/AU]; c/- Level 20, 570 Bourke Street, Melbourne, VIC 3000 (AU).

(74) Agent: **FREEHILLS CARTER SMITH BEADLE**; 101 Collins Street, Melbourne, VIC 3000 (AU).

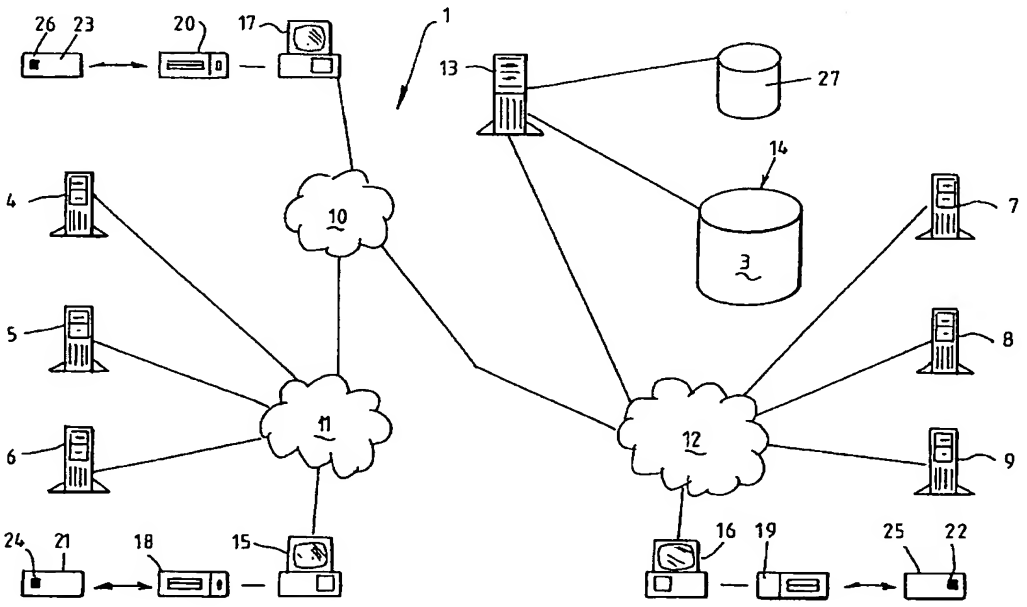
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: SECURE SYSTEM ACCESS



(57) Abstract: A method of managing access to secure resources (4-9), the method including: providing an schema of permission rights in respect of secure resources; and, delegating to one or more users an ability to delegate (32) a profile (31) of selected permission rights in respect of one or more secure resources.

WO 01/82092 A1

SECURE SYSTEM ACCESS

The invention relates to system access, and relates particularly though not exclusively to the management of secure environments for e-commerce systems.

The Internet, and more particularly the World Wide Web, has created new opportunities for conducting commercial transactions electronically. In this respect, electronic commerce between businesses (B2B e-commerce) is expected to become ever more pervasive. Accordingly, the ability of vendors to manage the process of identifying users and granting those users access to a vendor's Web site is increasingly problematic. Without an adequate system, a vendor cannot appropriately control who is permitted access to its systems. This risk exposure can potentially result in inappropriate system usage.

Existing access methods allow the user to access their vendor's secure Web site or network and conduct business electronically (such as over the Internet) through network to network connections. A user attempting to access a particular site for the purpose of a transaction must have corresponding software installed on their computer. An initial set up procedure is required for each new user of the software before they are granted permission to access the vendor's network.

This technique is relatively labour intensive. As a result, many of the efficiencies that might otherwise be achieved as a result of doing business electronically can be negated, due in large part to the inconvenience associated with system management.

Another approach is to link up the computer networks of two parties to facilitate e-commerce transactions. This can also be a costly and time-consuming practice, as external consultants are generally needed to facilitate such a connection, and significant costs are incurred from the increased labour and the need to purchase new software and hardware. Such methods are also unsuitable for B2C e-commerce due to the costs and expertise required. This approach also poses significant security risks for both parties in the event of one

end of the system becoming compromised, or the business relationship between the two parties becoming hostile. The ability of one party to cause damage to the other's systems is a tangible risk exposure for both parties.

In short, current methods are generally deficient as they involve a reasonably high amount of negotiation between parties, with consequent costs. Accordingly, it would be desirable to address these and other problems associated with existing systems and techniques relating to the administration of permission rights.

The Applicant has recognised that access to secure resources can be advantageously administered by allowing for the delegation of permission rights to one or more users who, in turn, are also able to delegate permission rights to other users. It is recognised that decentralised administration of permission rights can be advantageously combined with a centralised administration of the execution of those rights.

One aspect of the invention provides a method of managing access to secure resources, the method including:

providing an schema of permission rights in respect of secure resources; and,

delegating to one or more users an ability to delegate a profile of selected permission rights in respect of one or more secure resources.

Each of said profiles of permission rights may be centrally maintained in a central server. Moreover, one or more of the secure resources may be hosted remotely from the central server

Preferably, the schema of permission rights is a logical arrangement of different permission rights that have an implied hierarchial order. Preferably, the schema is extendable to allow the grant of permissions in relation to the secure resources. Preferably, the secure resources are either information sources or applications.

Preferably, at least a first of the users is able to delegate to another user a profile of selected permission rights which is less than or equal to the permission rights held by the first user.

Preferably, said central server grants or denies requests made by users in respect of said secure resources. Preferably, activities of users are centrally audited and tracked in the central server. Preferably, requests to the central server are referred by servers that receive requests from remote users.

Preferably, each of said profiles of permission rights represent a profile in respect of a particular set of one or more secure resources.

Preferably, said permission rights govern access to generally restricted information, or use of generally restricted functionality. Preferably, said secure resources are information-based or functionality-based resources, access to which is generally restricted subject to verification of access rights is respect of said resources.

Preferably, there is for each user and each secure resource an associated access right. That is, there is for each secure resource a set of access rights associated with respective users.

The Applicant has recognised that a neutral provider can advantageously act as a central hub for the administration of access rights to sensitive information stored on the servers of various organisations.

Another aspect of the invention provides a method of allowing secure access to a remote system via a network, the method including:

(a) storing in a central server a database of permission rights for a plurality of secure resources stored in one or more remote servers;

(b) receiving a request for access to one of said respective secure resources from said plurality of remote servers;

(c) establishing the identity of a user making said access request;

(d) determining whether the user has permission rights which are sufficient to allow the user to access said one secure resource; and

(e) approving or declining said access request if the permission rights of the user are or are not sufficient to allow the user to access said one secure resource.

Preferably, said request is made to one of said remote servers and is redirected from that remote server to said central server.

A further aspect of the invention provides a method of allowing secure access to a remote system via a network, the method including:

(a) receiving a request for access to a secure resource;

(b) establishing the identity of a user making said access request;

(c) determining whether the user has permission rights which are sufficient to allow the user to access the secure resource; and

(d) approving or declining said access request if the permission rights of the user are or are not sufficient to allow the user to access the secure resource;

wherein the secure resource is stored at a remote server, and requests for access to the secure resource are received at the remote server and redirected to a central server.

Preferably, upon approval of the access request, a second remote server directs the access request to a first remote server, and the first remote server responds to the user.

Preferably, establishing the identity of the user involves the use of identification codes such as, for example, digital certificates. Preferably the digital certifications use public key cryptography techniques. Preferably, one or more users with appropriate permission rights can issue their identification codes for other users. Preferably, those one or more users can specify the permission rights enjoyed by the other users for whom they issue identification codes.

Preferably, the secure resources are formatted in a manner specific to the user making the access request.

The described methods can be used to facilitate electronic commerce transactions, by allowing organisations to administer and establish their own hierarchy of permission rights for a number of users. Preferably, a software tool or wizard is provided for allowing the organisation to develop and manage these permission rights.

Preferably, users can be delegated the capability to issue digital identification certificates, including Identrus certificates, to other users.

Preferably, the secure server is capable of operating at a remote site and using digital certificates stored on a smart card to verify the permission rights of a third party.

In particular embodiments, it is preferred that a software application or component (such as, for example, a Java applet) can be downloaded onto a user's computer for the purpose of encoding a smart card with a public key and a private key. Permission rights are managed by an administrator with the appropriate permission level to grant appropriate access rights to users' smart cards.

The following description refers in more detail to the various features of the present invention. To facilitate an understanding of the invention, reference is made in the description to the accompanying drawings where the invention is illustrated in a preferred, but not limiting, embodiment.

In the drawings:

Fig. 1 is a schematic diagram of a system implementing the functionality of an embodiment of the invention;

Fig. 2 is a schematic diagram illustrating hierarchically ordered schemas of permission rights administered in the system of Fig. 1; and

Figs. 3 to 5 are flow diagrams illustrating the operation of various functionality of the system of Fig. 1.

Referring now to the drawings, a system 1 is provided in which a schema 2 of permission rights 3 is established to administer access to secure resources 4 to 9, such as particular resources (eg URLs) accessible from a computer network 10 to 12, and to which access is generally restricted.

The system 1 includes a central server 13 and a database 14 in which is stored, for each user, a profile of permission rights in relation to particular secure resources. These permission rights may be, for example, read/write/execute, or add/delete/modify/purchase or any other schema of permission rights that is appropriate. In this embodiment, the schema of permission rights is fully extensive and can be adapted as required in relation to specific secure resources. For example, when a secure application is provided,

various application-specific actions can be defined, and corresponding permission rights established. As a result, it is possible to determine the level and type of access a user has to any of those application-specific actions.

When a new user is created, that user 30 is provided the ability to create a further new user having a profile of permission rights that is at least equal to the profile of the creating user. Accordingly, new users are typically delegated:

(a) a profile 31 of permission rights in relation to the secure resources, as well as

(b) the ability to delegate 32 a profile of permission rights in relation to those secure resources.

In some cases, an administrative user 33 will only be delegated the ability to delegate profiles of permission rights to other users, without any or only minimal permission rights of their own. In other cases, a particular user 34 will only be granted a profile of permission rights without the ability to delegate profiles to other users.

The system 1 is intended to be used by organisations to allow any appropriate networked computing device to be used to add and delete users, and modify their permission and access / restriction levels and any other relevant criteria.

The system 1 allows authorised users, both internal and external to a particular organisation, to access secure resources or applications remotely from any computer or other access device, such as the terminals referenced 15 to 17 (for example, personal digital assistant). It is intended that each such computing device 15 to 17 is equipped with a smart card peripheral device 18 to 20 that is able to read and write information from and to a smart card 21 to 23. The smart card stores a private key and public key pair 24 to 26 for identification of the respective smart card user. Preferably the system 1 uses digital certificates such as Identrus certificates, to authenticate users.

The computing device 15 to 17 can be positioned in any location that provides satisfactory network access. Accordingly, the computing device can be remote from the remaining infrastructure of the system, allowing for remote

distribution of the system. Computing devices using the system desirably have a smart card device for use with implementations which store certificates on smart cards.

The profiles of permission rights represented in Figure 2 are organised on an application-by-application basis. Permission rights are granted on the basis of establishing a rule or "policy" for a particular action. Permission is only granted if a user has the appropriate attributes specified by the policy. If the user's permission profile does have appropriate attributes, header variables are passed to the application. These header variables contain name/value pairs corresponding with the given user. This header variable information is used to build / customise the user interface that is presented to that user.

A policy for a given application specifies what types of users (ie profiles of permission rights having particular attributes) can perform specified actions. Additionally, further information can be passed to the application, when and as required, to enable it to restrict the user's activity for any reason.

It should be noted that the attribute types such as view, maintain, drawdown, roll-over etc are all controlled by the application. The system's role is to match the user with these attributes. The system does not process a user's attributes. The system merely passes information to particular applications specifying the user, and the permissions that user has. This may be, for example, viewing and drawdown only.

To provide a further explanation of the system, a particular example is now described. Initially, a user ID and password combination (or, alternatively, a digital certificate) is stored on a hard drive of a particular computer or on a smart card 21 to 23. This forms the basis for identification. The system 1, however, is not implementation specific - various identification techniques can be incorporated into the system. Management of relationships and their permissions can be done from any computer as the smart card carries the digital certificate that provides the ID to the system, provided that the card has sufficient authority to perform the action.

A company (ABC Pty Ltd) contacts the system provider (Central Authority) for the purpose of implementing the system for ABC Pty Ltd's Web site. The Central Authority identifies the user, possibly using the system to identify ABC Pty Ltd through an Identrus certificate that ABC Pty Ltd sends to the Central Authority. All the security and access to the company's application is controlled and stored remotely on the Central Authority's server, including audit and non-repudiation functions.

ABC Pty Ltd then logs onto an online application form which is itself protected by the system. This application form allows ABC Pty Ltd access to the system. This process can occur electronically, as indicated in Fig. 3. Accordingly, at step 50, the administrator access a wizard feature accessible from the central server 13 and fills in the position levels that a new employee is to have. At step 51, the central server 13 checks the administrator's ID and their permission levels to confirm that they have authority to set up the new smart card with the specified access/permission levels. Permission is subsequently either denied at step 52 or, at step 53, the action is authorised. The administrator card is subsequently removed and the new employee smart card required to be encoded is inserted in the corresponding smart card reader at step 54. At step 55, the central server 13 provides data to the remote user terminal in question to enable the encoding of the new smart cart with the appropriate permission levels. At step 56, the administrator is then able to provide the new employee with their personal smart card. At step 57, the central server 13 then creates a new user within the particular company permissioning structure maintained in the database 14.

ABC Pty Ltd takes the system to their developers, who install the system to the front end of ABC Pty Ltd's Web system. During this process, the URL hierarchy, the database structure, application administrators, information regarding which URLs are protected as a secure resource and the business rules within the URLs, are loaded onto the database through one or more software "wizards" 27 or other tools.

The administrator (possibly the departmental heads) will build further screens for the users and set up the users with unique profiles of permission rights using other wizards. The users may be staff, or external customers. Each of the users are provided with a smart card (or a user ID and password combination) that will enable them to access certain restricted URLs of ABC Pty Ltd applications. Particular applications will allow certain users to create new profiles, and corresponding cards. The process of a user gaining access to secure resources is indicated in Fig. 4. A user logs onto ABC Pty Ltd's computer system. Requests for secure resources are intercepted at step 61 and re-routed through the system. The system 13 determines at step 62 whether the user has sufficient and appropriate permission rights to access the secure resources. Depending on the outcome, the request is either denied at step 63 or authorised at step 64.

As shown in Fig. 5, ABC Pty Ltd's customer (XYZ Pty Ltd) can take a smart card, and log onto ABC Pty Ltd's Web site at step 70 from any computer, irrespective of location. If XYZ Pty Ltd try to access one of ABC Pty Ltd's restricted URLs, the system intercepts the request at step 71, challenges the user's ID at step 72, and check it off against the profile of permission rights stored in the system database for that user at step 73.

The Central Authority's server 13 completes the risk management activities at a site remote from those of the sites of remotely hosted secure resources 4 to 6 and locally hosted secure resources 7 to 9. The secure server 13 effectively acts as a hub through which permission-based request for access to an organisation's secure resources must pass before permission to read/edit/delete etc the particular secure resource is granted or denied.

Each time a customer/staff member of a company wishes to access a secure resource 4 to 9 (such as, for example. a restricted access URL) to do something that requires a certain level of permission, an identification and authentication procedure is conducted.

The system 1 does not inherently limit the number of new users that can be issued permission rights. The system 1 also allows a first user to provide a

second user with a smart card or logon identification code which allows that second user access rights to the secure system which are equivalent to the first user. The system is safeguarded so that a first user cannot grant permission rights that are superior to those of the first user. Some exceptions to this general rule exist. For example, in some cases, it is desirable that administrative personnel do not have permission rights to run some applications, but have the authority to create new users that do have such permission rights.

The administrator at XYZ Pty Ltd may initially wish to authorise users within XYZ Pty Ltd or within an allied company to access ABC Pty Ltd's Web application. The process of doing this is analogous. The relevant personnel at XYZ Pty Ltd logs onto the system, which identifies and checks if they authorised to encode new cards for access to ABC Pty Ltd's application, and what level of permission rights they are authorised to allow on the issue of further cards.

ABC Pty Ltd can then market itself as having all its Web security protected by the Central Authority. The Central Authority thus effectively provides a risk management facility for ABC Pty Ltd. The system 1 also stores an audit and non-repudiation trail in the system database 14. Every B2B or B2C customer of ABC Pty Ltd can be assured that the privacy and security of their information and transactions is protected by the Central Authority's risk management system, which is held remotely to ABC Pty Ltd.

ABC Pty Ltd is also assured that they can always identify a user accessing secured resources on their Web site, and that user has been given access by one entitled to do so. ABC Pty Ltd can also be assured that they have non-repudiation of transactions undertaken through their Web site.

As the security access system 1 stores all relationships between users and permission rights, ABC Pty Ltd will also have the benefit of being able view a relationship tree displaying every user of their application and information on who authorised the access for that user. Reports of variable complexity and type can be generated in relation to the various secure resources and users.

XYZ Pty Ltd also has access to view their branch of the ABC Pty Ltd permissioning tree. Administrators at both companies can manage and prune their relationship trees or branches as the need arises.

The privacy of the transmitted information is encrypted to ensure that it is secure on route to its destination. ABC Pty Ltd can also decide which parts of their application they wish to keep private from both internal and external customers.

The system 1 enables companies to allow users to access their application on a screen by screen basis. Each user can be given permission to access one particular URL and not another, and to perform one particular action at that URL and not another.

The system database 14 maintains records of the activities of developers and administrators for audit and non-repudiation purposes. This can be used to check the integrity of the application and for dispute resolution purposes.

A master wizard 27 can be used by the administrator at ABC Pty Ltd to sequentially build other wizards for master users to add, delete and determine the level of access new and existing users will have.

Access to a company's application can be from any computer 15 to 17. A session cookie 74 is downloaded onto the system for the duration of the session enabling access to the application.

The security system 1 described herein provides users with the ability to have all the administration of a permissioning system conducted at a remote and secure site, or secure server. The secure server 13 allows permissions 3 to be created and stored at its remote site.

The system 1 is particularly suitable for administering the security of a business organisation's data against abuse and inadvertent misuse by that organisation's staff, as all activities are able to be monitored by a trusted third party. The system 1 is particularly suitable for information-intensive organisations which deal in sensitive data which is required to be maintained and manipulated by a large number of staff on a regular basis for the same reason. Accordingly, the system 1 is particularly suitable for financial

institutions such as banks, or other data-based organisations such as hospitals, or insurance companies.

Terminals 15 to 17 used by the organisation to administer secure information include smart card readers 18 to 20 which are able to read the contents of a smart card 22 to 24 used by relevant staff. The smart cards include a digital certificate 22 to 24 which identifies the respective staff member. The terminals and smart card readers may typically be within a single location, such as corporate headquarters, but may be just as easily be located through various offices, or off-site at, for example, a customer site. In short, terminals interfacing with the central server can be located anywhere on a network typically the Internet 10, LAN 11 and 12, or a virtual private network.

In one implementation, a staff member swipes the smart card through the reader at the start of any session, and computer software executing on the computing device records the public and private keys for use during the session. This computer software is preferably downloaded as required from the central server 13 and can thus be written, for example, as a Java• applet or application.

The system 1 enables the Central Authority to provide another business with the capability to use digital certificates (such as Identrus certificates) as a means of authenticating their users to other entities. This can be done remotely. As an example, ABC Pty Ltd can use the system to verify their identity.

Once the system 1 has confirmed the identify to ABC Pty Ltd, a digital certificate can be issued using the system, which can then identify that user to another entity with which they may wish to deal, such as XYZ Pty Ltd.

The responsibility of who within ABC Pty Ltd can perform this function rests with ABC Pty Ltd. The responsibility of the Central Authority is to be able to prove that the digital certificate was properly issued to an authorised user from the identified company, in this case ABC Pty Ltd. Effectively the Central Authority guarantees to XYZ Pty Ltd that ABC Pty Ltd is ABC Pty Ltd.

A further example of this process is to enable another organisation to issue certificates as a means of identifying themselves and other individuals. For example, the Central Authority may wish to licence out the certificate

issuing process to another company once the Central Authority has checked their internal and external procedures. This proxy organisation can then issue certificates to third parties to allow those third parties to identify themselves when engaging in electronic transactions.

Once the encrypted keys have been presented to the application, a permission test is conducted at the secure server. The request is then either approved and re-routed to the requested Web site / network or transferred to an alternate Web page or screen advising that approval to enter that site was not given.

As described above, the system 1 includes the capability to allow any organisation to issue digital certificates through a standard Web browser or smart card. The system 1 includes the ability to allow individual smart cards to generate public and private key pairs through a smart card reader/writer . As described, these public and private keys form the basis of identification of users for the administration of permission rights. It is preferred that permission attached to the first smart card issued to an organisation includes the capability to create further smart cards with varying permission profiles.

Thus the system 1 enables an organisation to manage and maintain its own permissioning structures 2. The encoding of each card issued by the organisation occurs at its discretion. The organisation will keep a track of the permissioning structure with the aid of software tool or wizard down to an individual level.

The system 1 also has the ability to customise the page depending on how a user wishes it to look. This information on how the smart card user wishes to view the page and what they view is also stored on the secure server and activated on initial logon. Upon gaining permission to view the site, the smart card communicates with the site and dictates how it should be viewed.

This feature enables the user to determine what information they need and makes the downloading of superfluous information unnecessary. This allows the browsing experience to be speeding up the process for the user.

The system 1 is designed to provide security and access to an organisation's applications. The system uses a variety of techniques to manage restricted access to these applications and resources.

It will be understood that the invention disclosed and defined in this specification extends to all alternative combinations of two or more of the individual features mentioned or evident from the text or drawings. All of these different combinations constitute various alternative aspects of the invention.

CLAIMS:

1. A method of managing access to secure resources, the method including: providing an schema of permission rights in respect of secure resources; and,

delegating to one or more users an ability to delegate a profile of selected permission rights in respect of one or more secure resources.

2. A method according to claim 1, wherein each of the profiles of permission rights is centrally maintained in a central server.

3. A method according to claim 2, wherein one or more of the secure resources are hosted remotely from the central server.

4. A method according to any one of the preceding claims, wherein the schema of permission rights is a logical arrangement of different permission rights that have an implied hierarchial order.

5. A method according to any one of the preceding claims, wherein the schema is extendable to allow the grant of permissions in relation to the secure resources.

6. A method according to any one of the preceding claims, wherein the secure resources include information sources or applications.

7. A method according to any one of the preceding claims, wherein at least a first of the users is able to delegate to another user a profile of selected permission rights which is less than or equal to the permission rights held by the first user.

8. A method according to any one of the preceding claims, wherein the central server acts to grants or denies requests made by the users in respect of said secure resources.

9. A method according to any one of the preceding claims, wherein activities of the users are centrally audited and tracked in the central server.

10. A method according to any one of the preceding claims, wherein requests to the central server are referred by servers that receive requests from remote users.

11. A method according to any one of the preceding claims, wherein each of said profiles of selected permission rights represents a profile in respect of a particular set of one or more secure resources.

12. A method according to any one of the preceding claims, wherein the permission rights govern access to generally restricted information or use of generally restricted functionality.

13. A method according to any one of the preceding claims, wherein the secure resources are information-based or functionality-based resources, access to which is generally restricted subject to verification of access rights in respect of said resources.

14. A method of allowing a secure access to a remote system via a network, the method including:

(a) storing in a central server a database of permission rights for a plurality of secure resources hosted at one or more remote servers;

(b) receiving an access request for access to one of the secure resources from one of the plurality of remote servers;

(c) establishing the identity of a user making the access request;

(d) determining whether the user has permission rights which are sufficient to allow the user to access the one secure resource; and

(e) approving or declining the access request if the permission rights of the user are or are not sufficient to allow the user to access the one secure resource.

15. A method according to claim 14, wherein the request is made to one of the remote servers and is redirected from that remote server to the central server.

16. A method of allowing secure access to a remote system via a network, the method including:

(a) receiving a request for access to a secure resource;

(b) establishing the identity of a user making said access request;

(c) determining whether the user has permission rights which are sufficient to allow the user to access the secure resource; and

(d) approving or declining said access request if the permission rights of the user are or are not sufficient to allow the user to access the secure resource;

wherein the secure resource is hosted at a remote server, and requests for access to the secure resource are received at the remote server and redirected to a central server.

17. A method according to claim 16 wherein, upon approval of the access request, a second remote server directs the access request to a first remote server, and the first remote server responds to the user.

18. A method according to either one of claims 16 or 17, wherein establishing the identity of the user involves the use of identification codes.

19. A method according to claim 18, wherein the identification codes comprise digital certificates.

20. A method according to claim 19, wherein the digital certifications use public key cryptography techniques.

21. A method according to any one of claims 16 to 20, wherein one or more of the users with appropriate permission rights can issue identification codes for other users.

22. A method according to claim 21, wherein said one or more of the users can specify the permission rights of the other users to whom identification codes are issued.

23. A method according to any one of claims 16 to 22, wherein the secure resources are formatted in a manner specific to the user making the access request.

24. A method according to any one of the preceding claims, and further including using a software tool or wizard to develop and manage the permission rights.

25. A method according to any one of the preceding claims, and further including delegating to one or more of the users the capability to issue digital identification certificates to other users.

26. A method according to claim 25, wherein the digital identification certificates include Identrus certificates.

27. A method according to either one of claims 25 or 26, wherein the secure server operates at a remote site and uses the digital certificates stored on a smart cart to verify the permission rights of a third party.

28. A method according to any one of the preceding claims, and further including downloading a software application or component onto a user's computer for the purpose of encoding a smart card with a public key and a private key.

29. A method according to claim 28, wherein the permission rights are managed by an administrator with the appropriate permission level to grant appropriate access rights to users' smart cards.

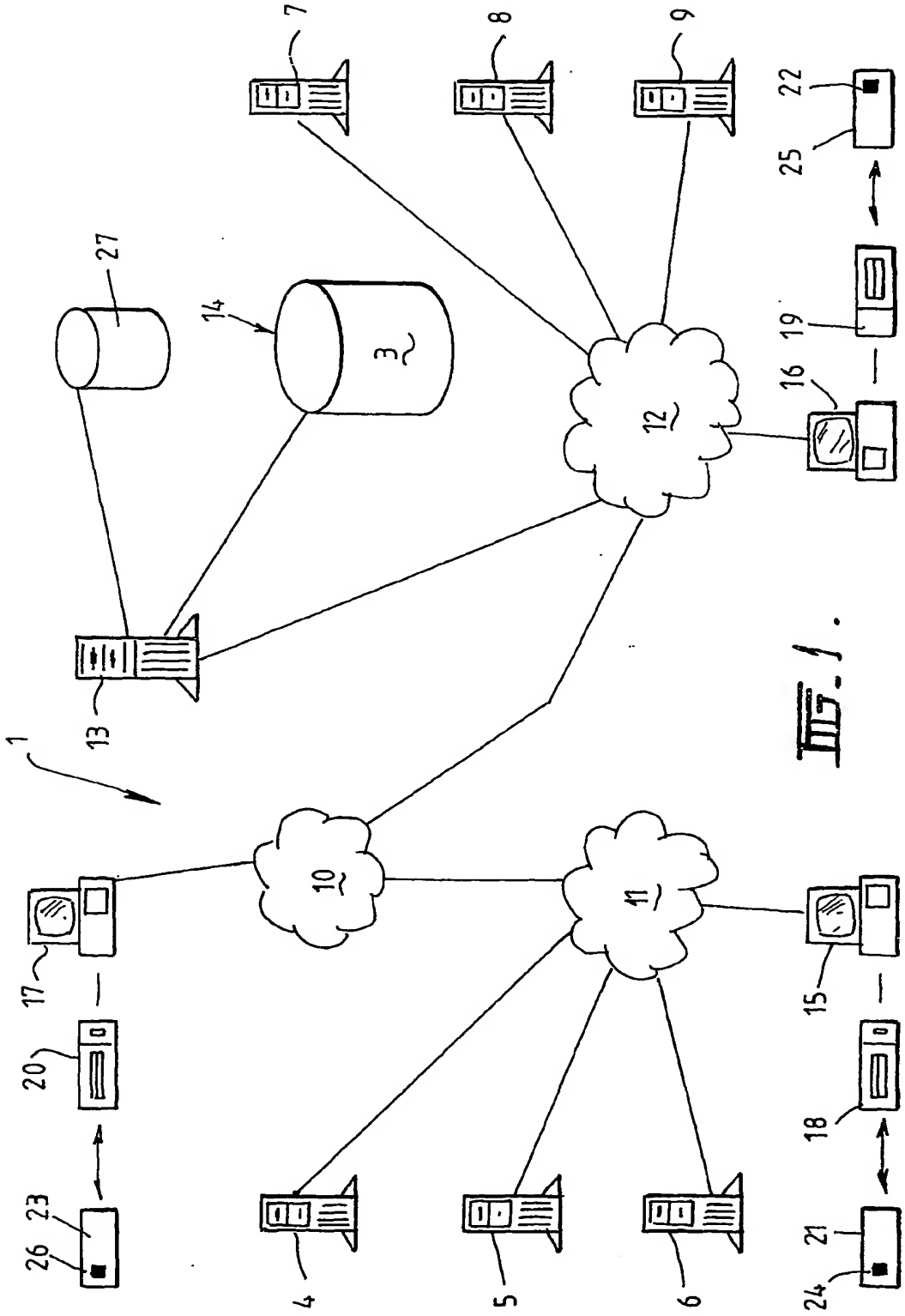


Fig. 1.

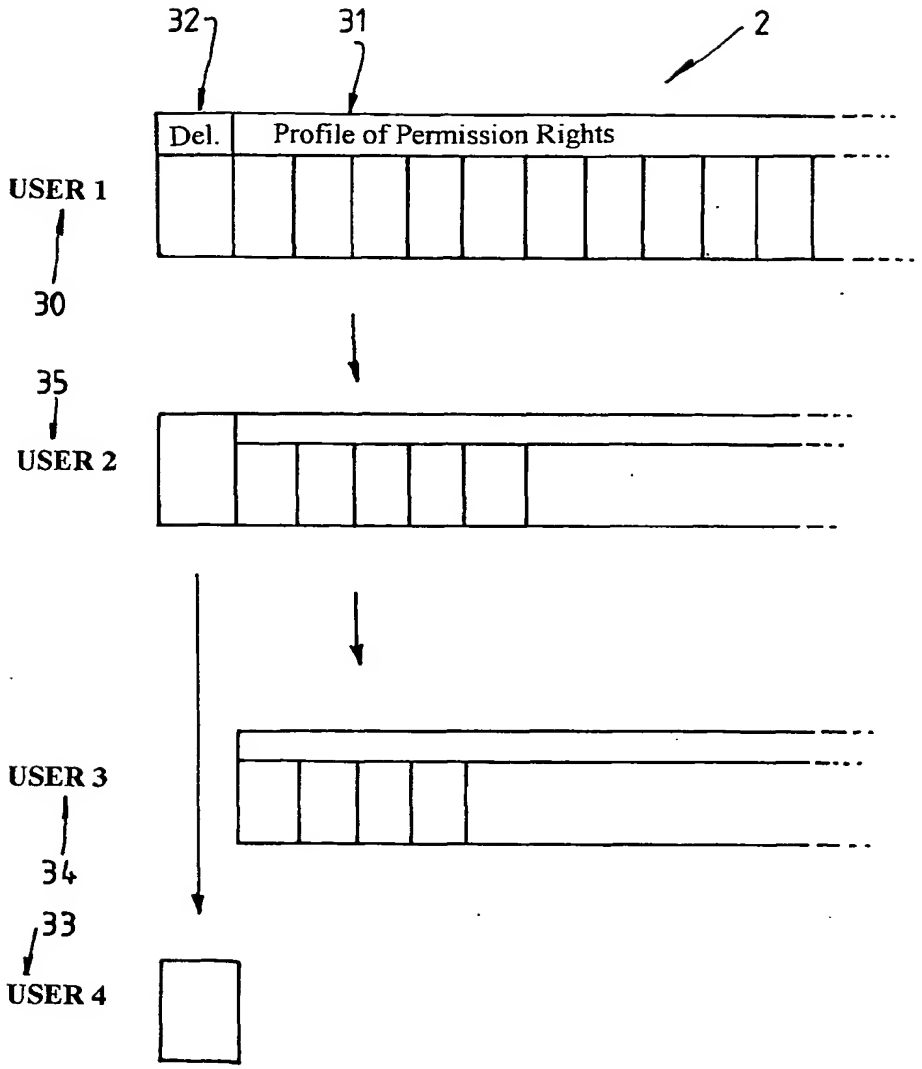
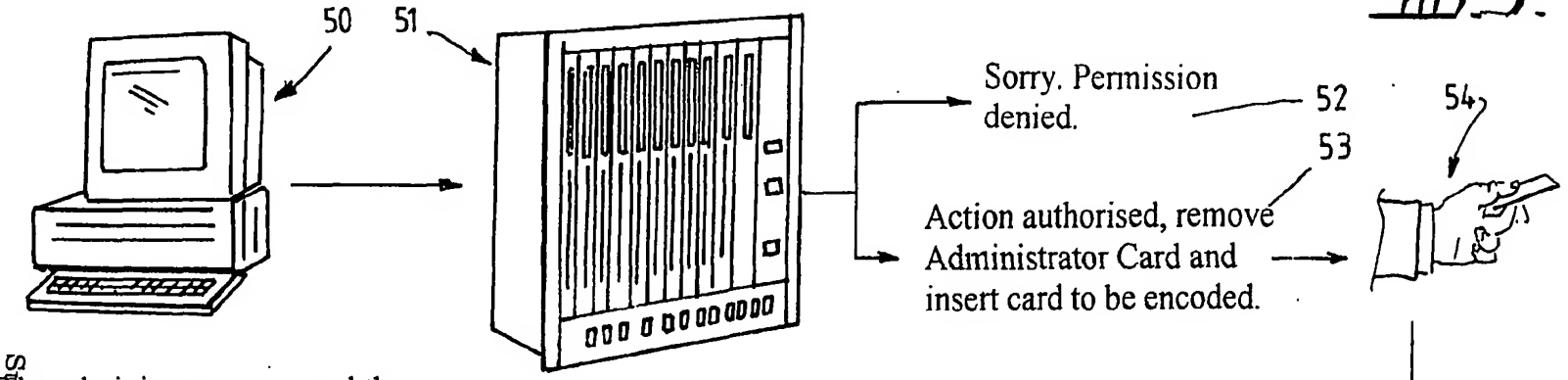

32
31
2
Del.
Profile of Permission Rights
USER 1
30
35
USER 2
USER 3
34
33
USER 4

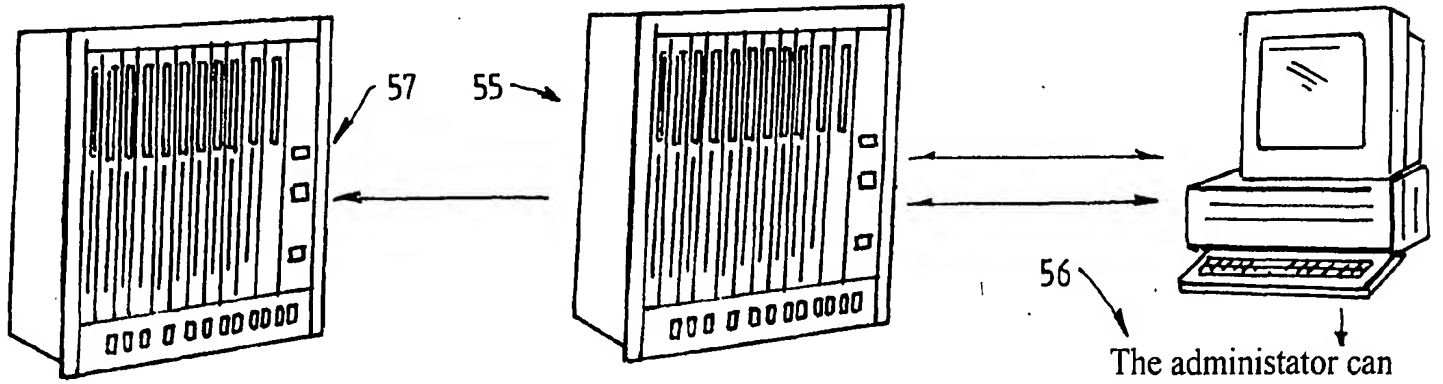
FIG. 2.

Fig. 3.



The administrator accessed the wizard feature stored on SAM and fills in the permission levels that the new employee is to have.

SAM checks the Administrator's ID and their permission levels to confirm that they have the authority to set up the new card with the specified access/permission level.



SAM now creates the new user within Company A's permissioning structure.

SAM then encodes the new card with the appropiate permission levels.

The administator can then provide the new employee with their personal Smart Card.

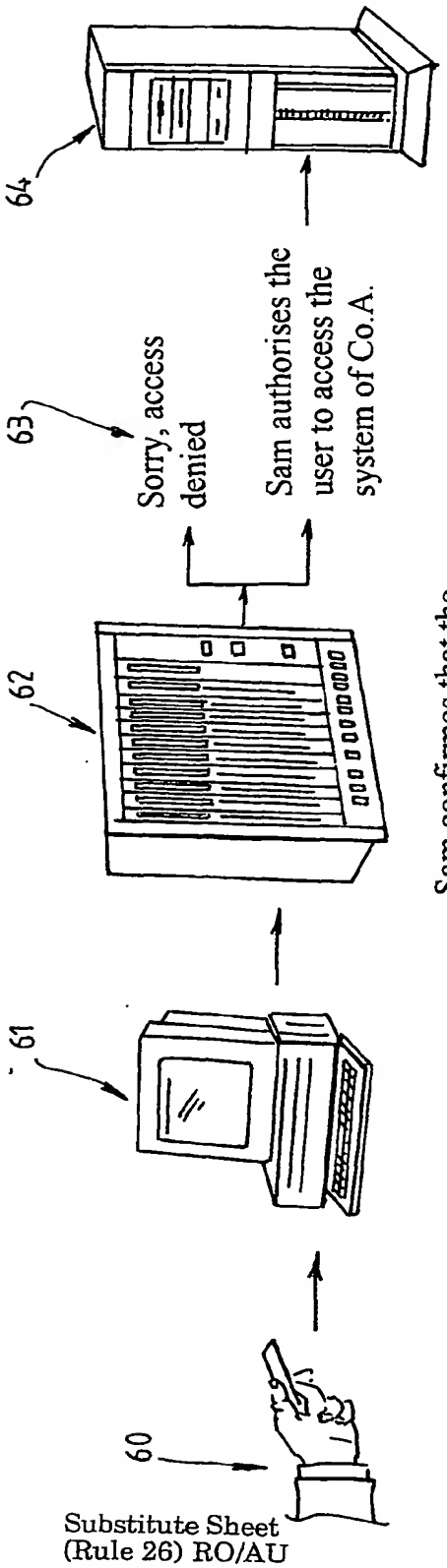
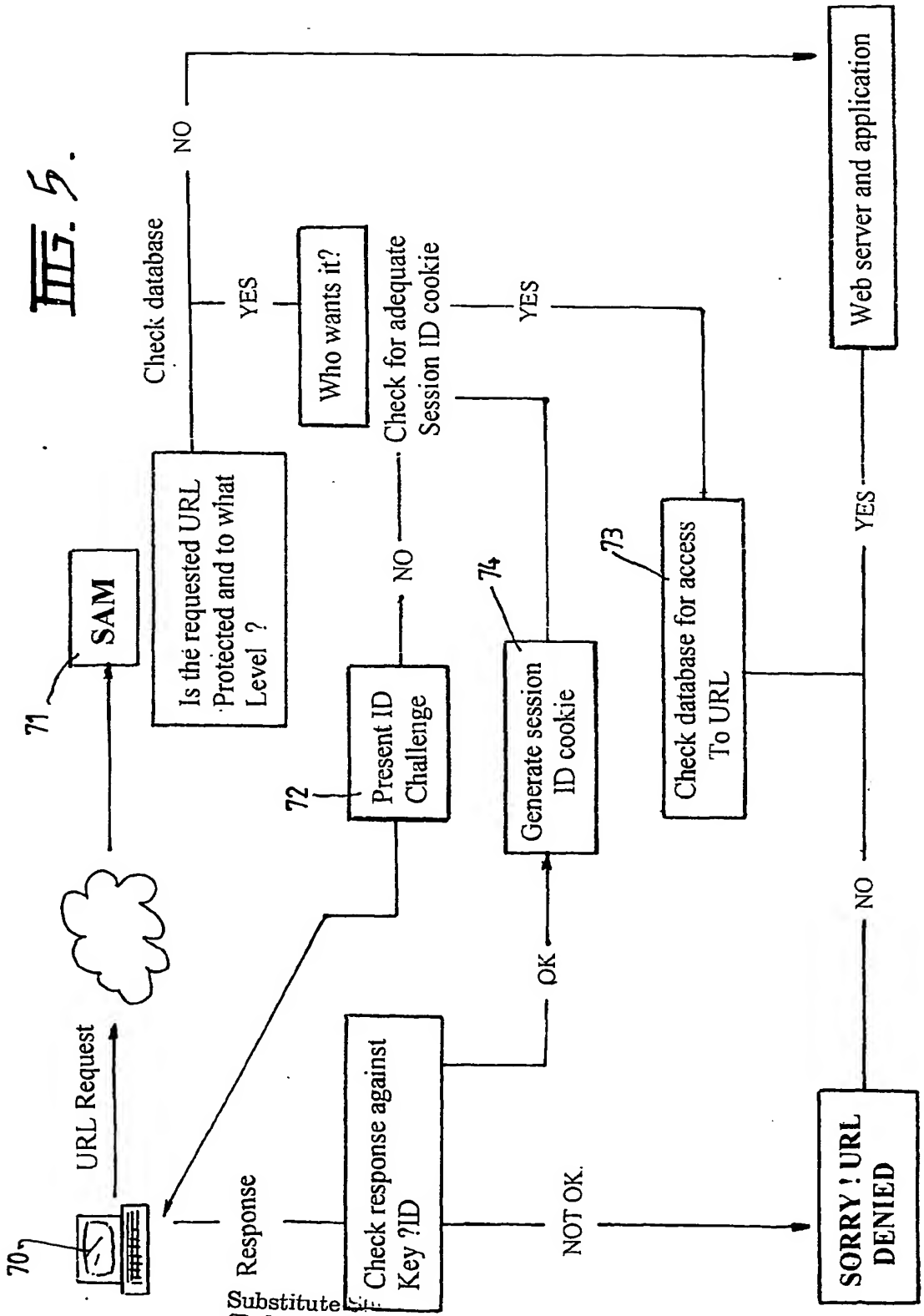

64
63
Sorry, access denied
Sam authorises the user to access the system of Co.A.
62
Sam confirmes that the smart card of the employee has sufficient permission to access the system.
61
60
A staff member of Company A inserts their smart card into the reader of any computer and logs on to their company's system. This request is intercepted and re-routed to SAM

Fig. 4.

FIG. 5.


70
URL Request
Response
71
SAM
Is the requested URL Protected and to what Level ?
Check database
NO
YES
Who wants it?
72
Present ID Challenge
Check response against Key ?ID
NOT OK.
OK
NO
Check for adequate Session ID cookie
YES
74
Generate session ID cookie
73
Check database for access To URL
YES
NO
Web server and application
SORRY ! URL DENIED

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU01/00451

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 15/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPAT, USPTO (KEYWORDS): NETWORK, INTERNET, SERVER, ADMINISTRAT+, PRIVILEG+, DELEGT+, HIERARCH+...

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98/40992 A (INTERNET DYNAMICS, INC) 17 September 1998 See whole document	1-29
X	EP 570683 A (INTERNATIONAL BUSINESS MACHINES CORPORATION) 24 November 1993 See whole document	14-29
A	US 5729734 A (PARKER et al) 17 March 1998 See whole document	

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 2001	24 July 2001
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized officer **Stephen Lee** Telephone No : (02) 6283 2205

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/AU01/00451

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	9840992	AU	64527/98	EP	966822	US	6105027
EP	570683	JP	6029993	US	5642515		
US	5729734	NONE					

END OF ANNEX